

CLAIMS

1. A method of securing packet data transferred between a first and second member of a private network over a backbone, the backbone operating according to a routing protocol, the method comprising the steps of:

5 encapsulating a private address of a packet from the first member in a public address of the packet to generate a tunneled packet;

transforming the tunneled packet by first applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet and then updating a field in the secure tunneled packet in accordance with the routing protocol of the
10 backbone.

2. The method according to claim 1, wherein the backbone comprises a plurality of provider devices, and wherein the steps of encapsulating and transforming are performed at one of the plurality of provider devices.

15 3. The method according to claim 1, wherein the steps of encapsulating and transforming are performed at an edge device disposed between the first member and the backbone.

20 4. The method according to claim 1, wherein the steps of encapsulating and transforming are performed at the first member.

25 5. The method according to claim 1, wherein the step of updating the field in the secure tunnel packet replaces a destination field associated with the private network with a destination field associated with the routing protocol of the backbone.

6. The method according to claim 1, wherein the group security association is associated with each member of the private network.

30 7. The method according to claim 1, further comprising the steps of:
each member of the private network registering with a global security server;

the global security server forwarding the group security association to each member of the private network.

8. The method according to claim 7 including the step of the global security server periodically forwarding a new group security association to each member of the private network.

9. A method of securing packet data transferred between a first and second member of a private network over a backbone, the backbone operating according to a routing protocol, the method comprising the steps of:

determining routing information associated with a packet received at the backbone according to the routing protocol of the backbone;
determining whether the packet is a member of the private network; and
modifying at least one field of the packet according to a routing protocol of the private network responsive to a determination that the packet is a member of the private network.

10. The method according to claim 9, wherein the step of modifying replaces a destination field associated with the routing protocol of the backbone with a destination field associated with a protocol of the private network.

11. An apparatus at a node for transforming packets for forwarding between a plurality of members over a backbone in a scalable private network, wherein the backbone operates according to a protocol, the apparatus comprising:

a key table, the key table including a security association for each private network that the node is a member;

a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address to provide a secured packet;

transform logic operable to apply a security association to each packet transmitted to the backbone, the transform logic including means for updating a field of the secure packet in accordance with a protocol of the backbone.

12. The apparatus of claim 11 wherein the means for updating the field replaces a destination field of the secured packet with a destination field corresponding to the protocol of the backbone.

5 13. A provider node in a backbone of a scalable private network, for transforming packets forwarded between a plurality of members of the scalable private network over the backbone, wherein the backbone operates according to a protocol, the provider node comprising:

10 a routing table, operable to determine a next hop routing address for each packet received at the provider node, the routing table operating responsive to a field of the packet arranged according to the protocol of the backbone; and

means for updating a field of the packet prior to the routing of the packet if it is determined that the packet is forwarded between members of the scalable private network.

15 14. The provider node of claim 13, wherein the means for updating replaces a destination field of the packet with a group identifier of the private network.

15. A system for providing secure packet transmission between members of a scalable private network over a backbone, the system comprising:

20 a first node, coupled to a backbone, the first node being a member of the private network and comprising:

a table for storing a group security association associated with the private network;

25 a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address to provide a secured packet;

30 transform logic operable to apply a security association to each packet transmitted to the backbone, the transform logic including means for updating a field of the secure packet in accordance with a protocol of the backbone; and

a provider node in the backbone operating according to a routing protocol,
the provider node comprising:

a routing table, operable to determine a next hop routing
address for each packet received at the provider node, the routing
table operating responsive to a field of the packet arranged
according to the protocol of the backbone; and

means for updating a field of the packet prior to the
routing of the packet if it is determined that the packet is forwarded
between members of the scalable private network.

5

10